

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004年12月9日 (09.12.2004)

PCT

(10) 国際公開番号
WO 2004/107339 A1

549293

(51) 国際特許分類: G11B 20/10, 20/12, G09C 1/00
(21) 国際出願番号: PCT/JP2004/006900
(22) 国際出願日: 2004年5月14日 (14.05.2004)
(25) 国際出願の言語: 日本語
(26) 国際公開の言語: 日本語
(30) 優先権データ: 特願2003-150906 2003年5月28日 (28.05.2003) JP
(71) 出願人(米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人(米国についてのみ): 海老原宗毅 (EBIHARA, Munetake) [JP/JP]. 勝股充 (KATSUMATA, Mitsuru) [JP/JP]. 久野浩 (KUNO, Hiroshi) [JP/JP]. 林隆道 (HAYASHI, Takamichi) [JP/JP].

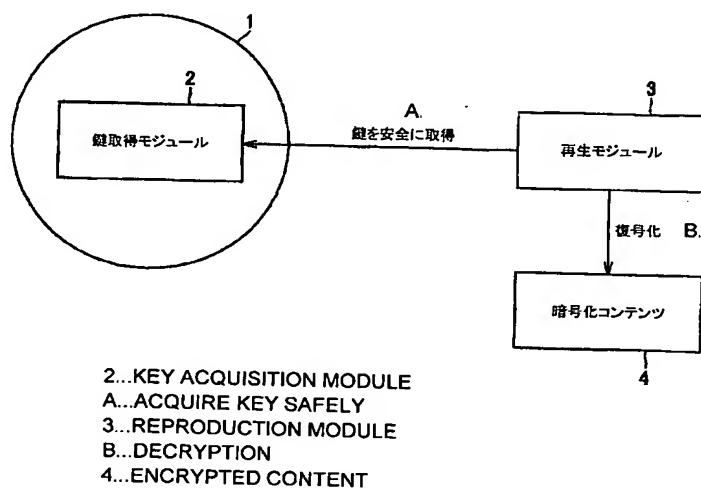
(74) 代理人: 中村友之 (NAKAMURA, Tomoyuki); 〒1050001 東京都港区虎ノ門1丁目2番3号虎ノ門第一ビル9階三好内外国特許事務所内 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

[続葉有]

(54) Title: INFORMATION RECORDING MEDIUM, INFORMATION PROCESSING DEVICE AND METHOD

(54) 発明の名称: 情報記録媒体、並びに情報処理装置及び方法



WO 2004/107339 A1

(57) Abstract: It is possible to prevent unauthorized copying of recorded information and flexibly operate a content. Furthermore, it is possible to facilitate improvement of the copy prevention technique. A key acquisition module (2) is recorded on an information medium (1) dedicated to reading and having the copy prevention technique. A reproduction module (3) safely acquires a key, inherent to the key acquisition module (2) from the key acquisition module (2), generates a content key from the medium resident on the information recording medium (1) while the reproduction module (3) and the encrypted content (4) need not be on the information recording medium (1) but may be outside the information recording medium (1).

(57) 要約: 記録された情報の不法コピーを防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする。鍵取得モジュール(2)は、コピー防止技術が施された読み取り専用の情報記録媒体(1)に記録されている。再生モジュール(3)は、この鍵取得モジュール(2)から該鍵取得モジュール(2)に固有のメディア鍵を安全に取得し、このメディア鍵からコンテンツ鍵を生成し、このコンテンツ

[続葉有]



SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF,

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

情報記録媒体、並びに情報処理装置及び方法

5 技術分野

本発明は、コンテンツの不正利用を防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする情報記録媒体、並びにそのような情報記録媒体を用いてコンテンツを再生する情報処理装置及びその方法に関する。

10

背景技術

近年において、光ディスク等の情報記録媒体の大容量化と普及により、記録されている情報の著作権を保護するために、不法なコピーの防止が重要とされてきている。すなわち、オーディオデータやビデオデータの場合には、コピー或いはダビングにより劣化のない複製物を容易に生成でき、またコンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる著作権の侵害等の弊害が生じてきているのが実情である。

このようなことから、上記不法コピーの防止を目的として、コピーコントロールCD (Copy Control Compact Disk ; CCCD) と称されるレッドブック規格外の音楽CDが開発・販売されるに至っている。このCCCDのセカンドセッションエリアに記録されているオーディオデータについては、CCCD上に記録されている専用の再生モジュールを用いてパーソナルコンピュータでの再生が可能であるものの、パーソナルコンピュータ内部へ取り込み（リッピング）ができず、コピーが防止されるようになされている。

また、同様に不法コピーの防止を目的として、SecuROM（登録商標）と称されるCD-ROM（Compact Disk - Read Only Memory）も開発・販売されている。このSecuROMでは、サブコード（Qサブチャンネル）に隠蔽されたコピー防止キーを抽出し、該コピー防止キーを用いて、少なくともその一部が暗号化されたアプリケーションを復号化することで、該アプリケーションを実行することができるものの、不法コピーされている場合には、アプリケーションを暗号化したコピー防止キーとは異なるものが抽出され、該アプリケーションを実行することができない（特開平11-250512号公報）。

しかしながら、このような従来のCCCDやSecuROM（登録商標）においては、媒体とそれに記録された音楽情報（コンテンツ）とが不可分であるため、コンテンツを媒体から切り離して運用することができず、運用の柔軟性がないという問題があった。また、媒体のコピー防止技術を改良しようとした場合、その媒体に記録されたコンテンツを再生するパーソナルコンピュータ等にインストールしなければならないソフトウェアが複雑化してしまう虞があった。

本発明は、このような従来の実情に鑑みて提案されたものであり、コンテンツの不正利用を防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする情報記録媒体、並びにそのような情報記録媒体を用いてコンテンツを再生する情報処理装置及びその方法を提供することを目的とする。

発明の開示

上述した目的を達成するために、本発明に係る情報記録媒体は、第1の実行ファイルが複製不可に記録された情報記録媒体であり、この第1の実行ファイルは、第2の実行ファイルとの間で認証処理を行う認証手

段と、該第1の実行ファイルに固有の固有鍵情報を取得する鍵取得手段と、上記固有鍵情報を上記第2の実行ファイルに送信する送信手段とを有し、情報記録媒体が情報処理装置に挿入されたときに実行されるものである。

5 このような情報記録媒体に記録された第1の実行ファイルは、情報記録媒体が情報処理装置に挿入されたときに実行され、第2の実行ファイルとの間で相互に認証処理を行い、第1のファイルに固有の固有鍵情報を第2のファイルに送信する。

また、上述した目的を達成するために、本発明に係る情報処理装置は、
10 第1の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置であって暗号化されたコンテンツを再生する第2の実行ファイルを有し、この第2の実行ファイルは、上記第1の実行ファイルとの間で認証処理を行う認証手段と、上記第1の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成手段と、上記暗号鍵情報を用いて上記暗号化されたコンテンツを復号化する復号化手段と、復号化した上記コンテンツを再生する再生手段とを有し、上記情報記録媒体が挿入されたときに実行されるものである。

このような情報処理装置が有する第2の実行ファイルは、第1の実行ファイルが複製不可に記録された情報記録媒体が挿入されたときに実行され、第1の実行ファイルとの間で相互に認証処理を行い、第1のファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生する。

また、上述した目的を達成するために、本発明に係る情報処理方法は、第1の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置の情報処理方法であり、上記第1の実行ファイルとの間で認証処理を行う認証工程と、上記第1の実行ファイルから取得した固有

鍵情報に基づいて暗号鍵情報を生成する鍵生成工程と、上記暗号鍵情報を用いて暗号化されたコンテンツを復号化する復号化工程と、復号化した上記コンテンツを再生する再生工程とを有するものである。

このような情報処理方法では、情報記録媒体に記録された第1の実行

5 ファイルとの間で相互に認証処理を行い、第1のファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生する。

図面の簡単な説明

10 第1図は、本実施の形態の概念構成を説明する図である。

第2図は、鍵取得モジュールがメディア鍵を取得して再生モジュールに転送するまでの処理の一例を説明するフローチャートである。

第3図は、鍵取得モジュールがメディア鍵を取得して再生モジュールに転送するまでの処理の他の例を説明するフローチャートである。

15 第4図は、再生モジュールが鍵取得モジュールから鍵を取得し、暗号化コンテンツを復号化して再生するまでの処理を説明するフローチャートである。

第5図は、再生モジュールが鍵取得モジュールから鍵を取得し、暗号化コンテンツを情報処理装置にインポートするまでの処理を説明するフ

20 ローチャートである。

第6図は、本実施の形態における情報処理装置の構成例を示す図である。

発明を実施するための最良の形態

25 以下、本発明を適用した具体的な実施の形態について、図面を参照しながら詳細に説明する。

先ず、本実施の形態の概念構成について、第1図を用いて説明する。第1図において、鍵取得モジュール2（第1の実行ファイル）は、コピー防止技術が施された読み取り専用の情報記録媒体1に記録されている。このコピー防止技術としては、例えばSecuROM（登録商標）に用いられている技術や、いわゆるダミーファイル法の技術が挙げられるが、これらに限定されず種々の技術を用いることができる。再生モジュール3（第2の実行ファイル）は、この鍵取得モジュール2から該鍵取得モジュール2に固有のメディア鍵（固有鍵情報）を安全に取得し、このメディア鍵からコンテンツ鍵（暗号鍵情報）を生成し、このコンテンツ鍵を用いて暗号化コンテンツ4を復号化して再生する。

このように、本実施の形態では、コンテンツが暗号化された状態で提供され、その暗号化コンテンツ4の復号化に用いられるメディア鍵がコピー防止技術の施された情報記録媒体1に記録されているため、暗号化コンテンツ4がコピーされた場合であっても正規の情報記録媒体1がなければメディア鍵を取得できず、コンテンツを利用することができない。

ここで、本実施の形態における鍵取得モジュール2は情報記録媒体1上に存在する必要があるが、再生モジュール3及び暗号化コンテンツ4は情報記録媒体1上に存在する必要はなく、情報記録媒体1の外部に存在していても構わない。つまり、再生モジュール3及び暗号化コンテンツ4の配置形態としては、

- 1) 情報記録媒体1上に再生モジュール3及び暗号化コンテンツ4が存在する場合、
- 2) 情報記録媒体1の外部に再生モジュール3及び暗号化コンテンツ4が存在する場合、
- 25 3) 情報記録媒体1上に再生モジュール3が存在し、情報記録媒体1の外部に暗号化コンテンツ4が存在する場合、

4) 情報記録媒体1の外部に再生モジュール3が存在し、情報記録媒体1上に暗号化コンテンツ4が存在する場合、の4通りが考えられる。

以下では、再生モジュール3及び暗号化コンテンツ4が情報記録媒体1の挿入される情報処理装置に存在する場合（上記2の場合）について、

5) 主として説明する。この再生モジュール3及び暗号化コンテンツ4は、予めネットワークを介して情報処理装置にダウンロードしたものであっても構わない。なお、以下では、情報記録媒体1は読み出し専用の光ディスクであるものとする。

先ず、情報記録媒体1のコピー防止技術としてSecuROM（登録10商標）の技術が用いられている場合に、鍵取得モジュール2がメディア鍵を取得し、このメディア鍵を再生モジュール3に転送するまでの処理を第2図のフローチャートに示す。

このSecuROM（登録商標）の技術とは、簡単には、予め情報記録媒体1上の所定のアドレス及び個数のサブコード（Qサブチャンネル）を変更しておき、アプリケーションを暗号化するコピー防止キーとしてその変更パターンを用いるものである。アプリケーションを実行する際には、上記所定のアドレス及び個数のQサブチャンネルを検索し、その変更パターンからコピー防止キーを抽出する。ここで、情報記録媒体1をコピーした場合、変更が施されていた正規でないQサブチャンネルは正規のQサブチャンネルとしてコピーされる。この結果、元々アプリケーションを暗号化していたものとは異なるコピー防止キーが抽出されることとなり、アプリケーションを復号化して実行することができない。なお、この第2図に示すコピー防止技術については、例えば特開平20-250512号公報に記載されている。

25) 具体的には、始めに第2図のステップS1において、鍵取得モジュール2は、暗号化されていない例えば前半部分のプログラムにより、情報

記録媒体 1 上の所定のアドレス及び個数のサブコード（Qサブチャンネル）をスキャンし、ステップ S 2において、そのQサブチャンネルが正規であるか否かを検索する。次にステップ S 3において、鍵取得モジュール 2 は、正規でないQサブチャンネルの数に応じてコピー防止キーを抽出する。そしてステップ S 4では、抽出したコピー防止キーを用いて鍵取得モジュール 2 の後半部分の暗号を復号化できるか否かが判別される。ステップ S 4において復号化できる場合（Yes）にはステップ S 5 に進み、復号化できない場合（No）には処理を終了する。ステップ S 5において、鍵取得モジュール 2 は、再生モジュール 3との間で認証処理を行い、ステップ S 6 では、認証の適否が判別される。ステップ S 6において相互に認証しない場合（No）には処理を終了し、相互に認証する場合（Yes）にはステップ S 7においてメディア鍵を再生モジュール 3 に転送する。

一方、情報記録媒体 1 のコピー防止技術としていわゆるダミーファイル法の技術が用いられている場合に、鍵取得モジュール 2 がメディア鍵を取得し、このメディア鍵を再生モジュール 3 に転送するまでの処理を第 3 図のフローチャートに示す。

このダミーファイル法の技術とは、簡単には、情報記録媒体 1 のサイズよりも大きいダミーファイルが実際に情報記録媒体 1 に記録されているかのように予めディレクトリレコードを変更しておき、アプリケーションを実行する際にそのダミーファイルのサイズを検査するものである。この情報記録媒体 1 をコピーする場合には、例えばディレクトリレコードのダミーファイルサイズを実際のダミーファイルのサイズに一致させる必要があるが、アプリケーションの実行前にそのダミーファイルのサイズが元のサイズ（情報記録媒体 1 のサイズよりも大きいサイズ）と一致するか否かが検査され、一致しない場合にはアプリケーションの実行

が許可されない。なお、この第3図に示すコピー防止技術については、例えば特開2001-229019号公報に記載されている。

具体的には、始めに第3図のステップS10において、鍵取得モジュール2はダミーファイルを開き、ステップS11において、そのダミーファイルのファイルサイズを検査する。次にステップS12において、鍵取得モジュール2は、そのファイルサイズが元のファイルサイズと一致するか否かを判別し、一致しない場合(No)には処理を終了する。一方、一致する場合(Yes)にはステップS13に進む。ステップS13において、鍵取得モジュール2は、再生モジュール3との間で認証処理を行い、ステップS14では、認証の適否が判別される。ステップS14において相互に認証しない場合(No)には処理を終了し、相互に認証する場合(Yes)にはステップS15においてメディア鍵を再生モジュール3に転送する。

次に、再生モジュール3が鍵取得モジュール2から鍵を取得し、暗号化コンテンツ4を復号化して再生するまでの処理を第4図のフローチャートに示す。ステップS20において、再生モジュール3は、鍵取得モジュール2がロード可能であるか否かを判別し、ロード可能でない場合(No)には処理を終了し、ロード可能である場合(Yes)にはステップS21に進む。次にステップS21において、再生モジュール3は、鍵取得モジュール2との間で認証処理を行い、ステップS22では、認証の適否が判別される。ステップS22において相互に認証しない場合(No)には処理を終了し、相互に認証する場合(Yes)にはステップS23において鍵取得モジュール2からメディア鍵を取得する。

続いてステップS24において、再生モジュール3は、取得したメディア鍵からコンテンツ鍵を生成し、ステップS25において、このコンテンツ鍵を用いて暗号化コンテンツ4の復号化を行う。なお、この暗号

化コンテンツ 4 は、情報記録媒体 1 が挿入される情報処理装置内に存在するものであっても、ネットワークを介してダウンロードしたものであっても構わない。そしてステップ S 2 6 において、コンテンツを再生可能であるか否かが判別され、再生不可である場合 (No) には処理を終了し、再生可能である場合 (Yes) にはステップ S 2 7 でコンテンツを再生する。

なお、上述した第 4 図では、暗号化コンテンツ 4 を再生する場合について説明したが、情報記録媒体 1 に暗号化コンテンツ 4 が記録されている場合には、この暗号化コンテンツ 4 を情報処理装置にインポートすることも可能である。このような場合において、再生モジュール 3 が鍵取得モジュール 2 から鍵を取得し、暗号化コンテンツ 4 を情報処理装置にインポートするまでの処理を第 5 図のフローチャートに示す。なお、ステップ S 3 4 においてコンテンツ鍵を生成するまでの処理は上述した第 4 図と同様であるため説明を省略する。

ステップ S 3 5 において、再生モジュール 3 は、生成したコンテンツ鍵を用いて、例えば暗号化コンテンツ 4 に付属する権利情報及び暗号署名のうち、暗号署名を復号化して権利情報の検証を行う。なお、この権利情報及び暗号署名は、情報記録媒体 1 上に存在するものであっても、ネットワークを介してダウンロードしたものであっても構わない。そしてステップ S 3 6 において、インポートが許可されるか否かが判別され、インポートが許可されない場合 (No) には処理を終了し、インポートが許可される場合 (Yes) にはステップ S 3 7 で暗号化コンテンツ 4 をインポートする。

以下、上述した情報処理装置の具体的な構成例について第 6 図を用いて説明する。第 6 図に示すように、情報処理装置 1 0 は、該情報処理装置 1 0 の各部を統括して制御する C P U (Central Processing

Unit) 11と、不揮発性のメモリであるROM (Read Only Memory) 12と、揮発性のメモリであるRAM (Random Access Memory) 13と、通信処理を行う通信部14と、図示しないハードディスクに対して各種データの書き込み及び／又は読み出しを行うHDD (Hard Disk Drive) 15と、音声を出力する出力部16と、情報記録媒体1に対して各種データの書き込み及び／又は読み出しを行なうインターフェース (I/F) 部17とがバス18を介して相互に接続されてなる。

CPU11は、例えばROM12に記録されているプログラムに従つて、プログラムを実行するための制御を行う。RAM13には、CPU 11が各種処理を実行する上で必要なプログラムやデータが必要に応じて一時的に格納される。

通信部14は、例えばモ뎀やターミナルアダプタ等により構成され、電話回線を介してインターネットに接続される。

HDD15は、図示しないハードディスクからデータの読み出しを行うほか、例えば通信部14を介して入力したデータの書き込みを行う。

オーディオ出力部16は、例えば通信部14を介して入力したオーディオデータや、インターフェース部17を介して情報記録媒体1から入力したオーディオデータに対して、必要に応じて変換を施して出力する。

インターフェース部17は、CPU11の制御のもとに、情報記録媒体1に対してデータを入出力するタイミングを調整し、データの形式を変換する。

このような情報処理装置10において、再生モジュール3は、例えばHDD15に記録されており、情報記録媒体1に記録された鍵取得モジュール2との間で上述した処理を行い、メディア鍵を取得する。そして、再生モジュール3は、このメディア鍵からコンテンツ鍵を生成し、このコンテンツ鍵を用いて、例えば通信部14を介して入力してHDD15

に記録された暗号化コンテンツ4を復号化する。復号化されたコンテンツは、CPU11の制御のもと、オーディオ出力部16から出力される。

以上説明したように、本実施の形態における情報記録媒体1及び情報処理装置10によれば、コンテンツが暗号化された状態で提供され、そ

5 の暗号化コンテンツ4の復号化に用いられるメディア鍵がコピー防止技術の施された情報記録媒体1に記録されているため、暗号化コンテンツ4がコピーされた場合であっても正規の情報記録媒体1がなければメディア鍵を取得できず、コンテンツを利用することができない。これにより、コンテンツの保護が図られる。

10 特に、暗号化コンテンツ4は情報記録媒体1上に存在する必要はなく、情報記録媒体1の外部に存在していても構わないため、情報記録媒体1の購入者のみが復号化できるような暗号化コンテンツ4をネットワークを介して配布するなど、コンテンツの柔軟な運用が可能となる。

15 また、再生モジュール3は、鍵取得モジュール2からメディア鍵を取得し、そのメディア鍵からコンテンツ鍵を生成して暗号化されたコンテンツを復号化するのみであり、情報記録媒体1にどのようなコピー防止技術が施されているかには依存しないため、コピー防止技術を改良した場合に、情報処理装置10に新たなソフトウェア等をインストールする必要がない。

20 なお、本発明は上述した実施の形態のみに限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能であることは勿論である。

25 例えば、上述の実施の形態では、コンテンツがオーディオデータであるものとして説明したが、これに限定されるものではなく、ビデオデータなど他種のデータであっても構わない。

以上詳細に説明したように、本発明に係る情報記録媒体、並びに情報処理装置及びその方法によれば、情報記録媒体に複製不可に記録された第1の実行ファイルと第2の実行ファイルとの間で相互に認証処理を行った後、第1の実行ファイルから第2の実行ファイルに固有鍵情報を送
5 信し、第2の実行ファイルでは、この固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生することにより、コンテンツの不正利用が防止されると共に、コンテンツの柔軟な運用が可能となり、さらにコピー防止技術の改良も容易となる。

請求の範囲

1. 第1の実行ファイルが複製不可に記録された情報記録媒体であつて、
- 5 上記第1の実行ファイルは、第2の実行ファイルとの間で認証処理を行う認証手段と、該第1の実行ファイルに固有の固有鍵情報を取得する鍵取得手段と、上記固有鍵情報を上記第2の実行ファイルに送信する送信手段とを有し、上記情報記録媒体が情報処理装置に挿入されたときに実行される
- 10 ことを特徴とする情報記録媒体。
2. 上記固有鍵情報は、コンテンツを暗号化する暗号鍵情報を暗号化するために用いられることを特徴とする請求の範囲第1項記載の情報記録媒体。
3. 上記第2の実行ファイル又は上記コンテンツは、上記情報記録媒体、上記情報処理装置又は他の情報処理装置に記録されていることを特徴とする請求の範囲第2項記載の情報記録媒体。
- 15 4. 上記コンテンツは、上記情報記録媒体に記録されており、上記固有鍵情報は、上記コンテンツに付属する署名情報を暗号化する暗号鍵情報を暗号化するために用いられ、
- 20 5. 上記送信手段は、上記署名情報に基づいて上記コンテンツを上記第2の実行ファイルに送信することを特徴とする請求の範囲第3項記載の情報記録媒体。
6. 第1の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置であつて、
- 25 暗号化されたコンテンツを再生する第2の実行ファイルを有し、

上記第2の実行ファイルは、上記第1の実行ファイルとの間で認証処理を行う認証手段と、上記第1の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成手段と、上記暗号鍵情報を用いて上記暗号化されたコンテンツを復号化する復号化手段と、復号化した

5 上記コンテンツを再生する再生手段とを有し、上記情報記録媒体が挿入されたときに実行される

ことを特徴とする情報処理装置。

6. 上記暗号化されたコンテンツは、上記情報記録媒体、上記情報処理装置又は他の情報処理装置に記録されていることを特徴とする請求の

10 範囲第5項記載の情報処理装置。

7. 上記暗号化されたコンテンツは、上記情報記録媒体に記録されており、

上記固有鍵情報は、上記暗号化されたコンテンツに付属する署名情報を暗号化する暗号鍵情報を暗号化するために用いられ、

15 上記第2の実行ファイルは、上記署名情報に基づいて上記第1の実行ファイルから上記暗号化されたコンテンツを受信する受信手段を有することを特徴とする請求の範囲第6項記載の情報処理装置。

8. 第1の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置の情報処理方法であって、

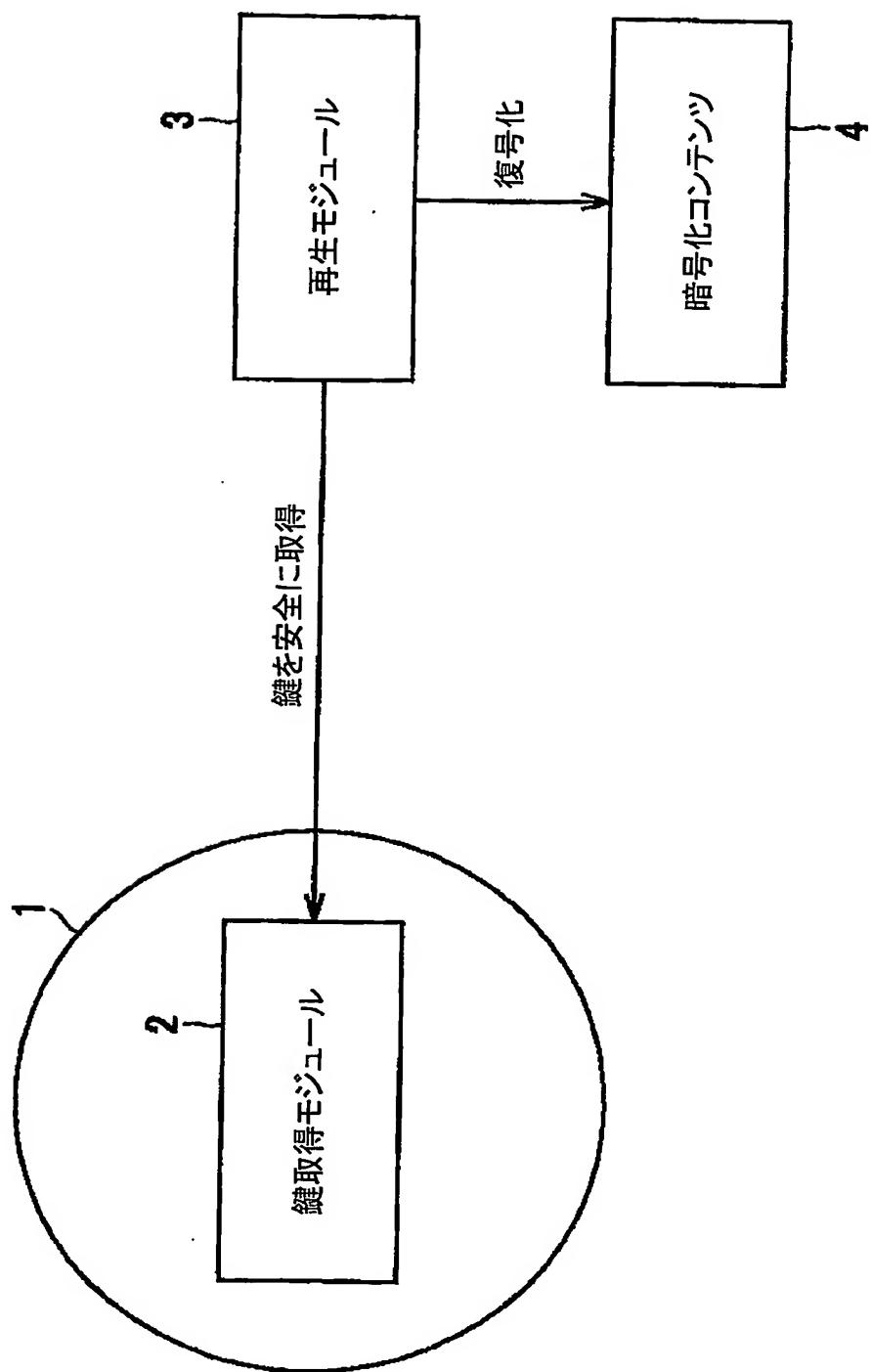
20 上記第1の実行ファイルとの間で認証処理を行う認証工程と、

上記第1の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成工程と、

上記暗号鍵情報を用いて暗号化されたコンテンツを復号化する復号化工程と、

25 復号化した上記コンテンツを再生する再生工程と
を有することを特徴とする情報処理方法。

1/6



2/6

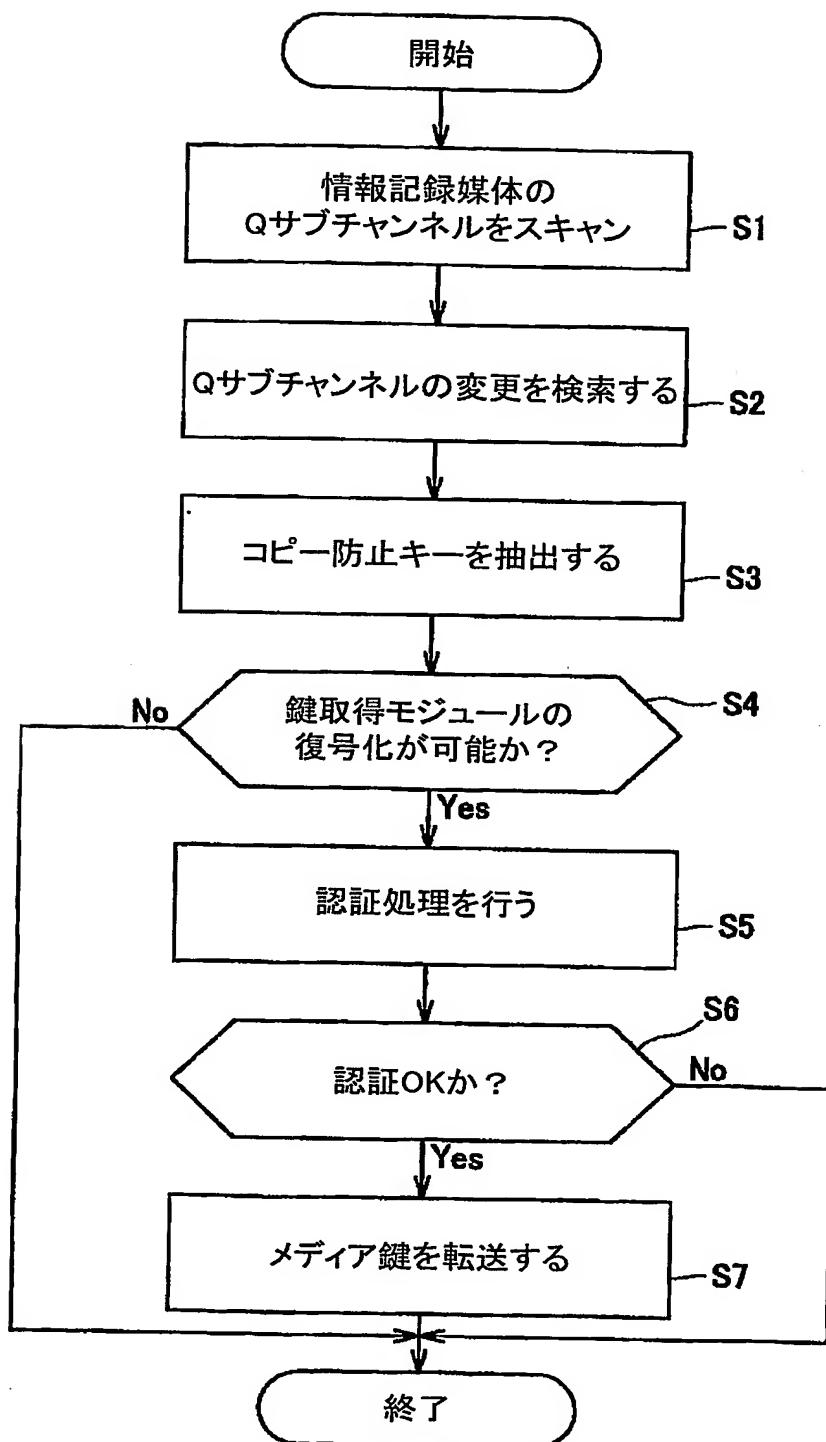


Fig.2

3/6

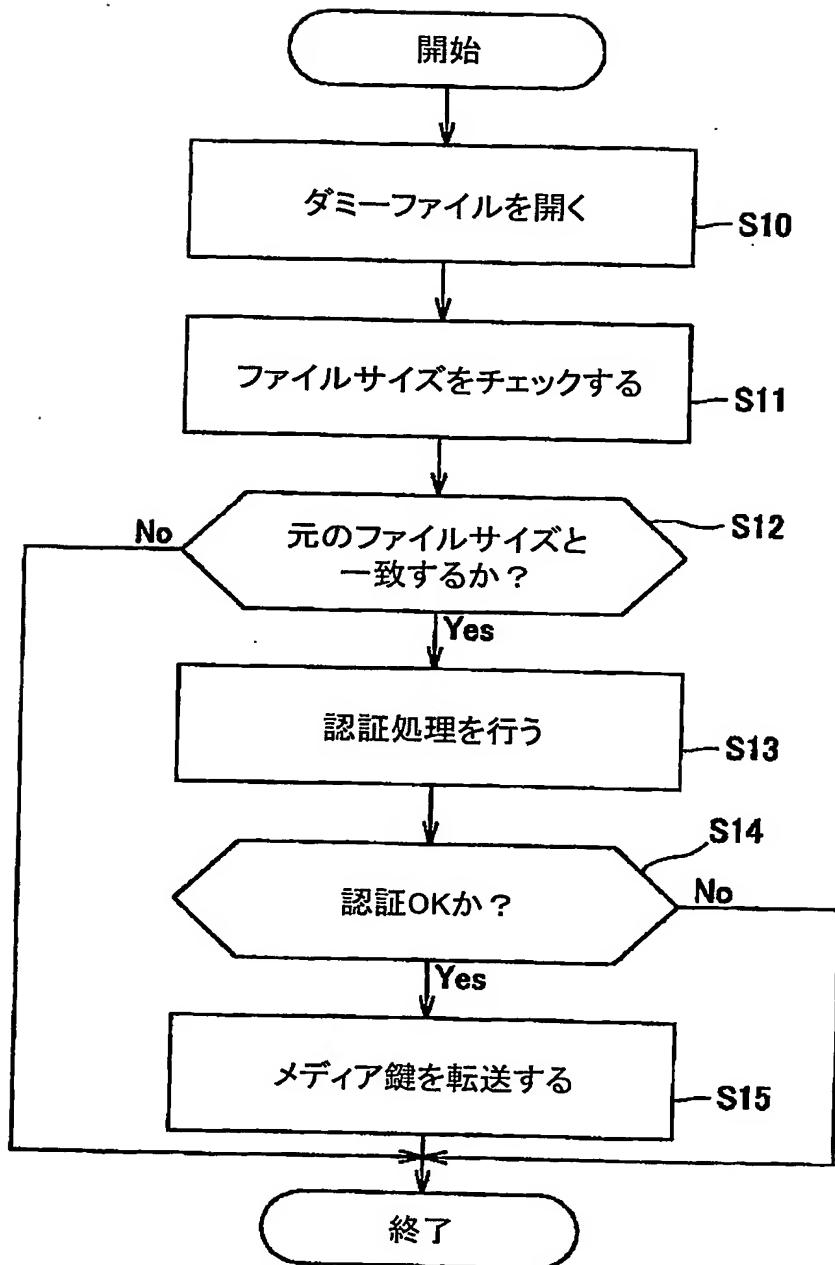


Fig.3

4/6

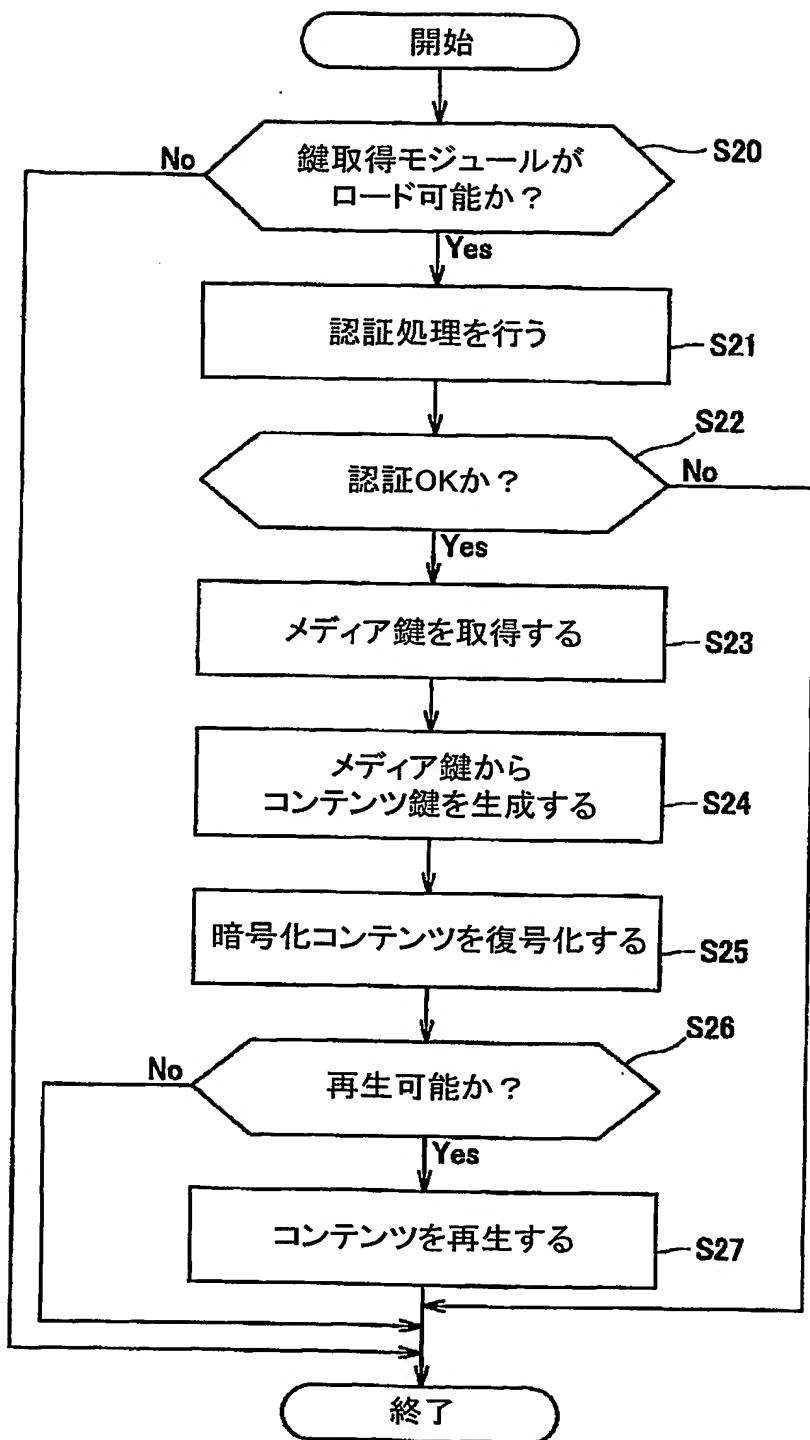


Fig.4

5/6

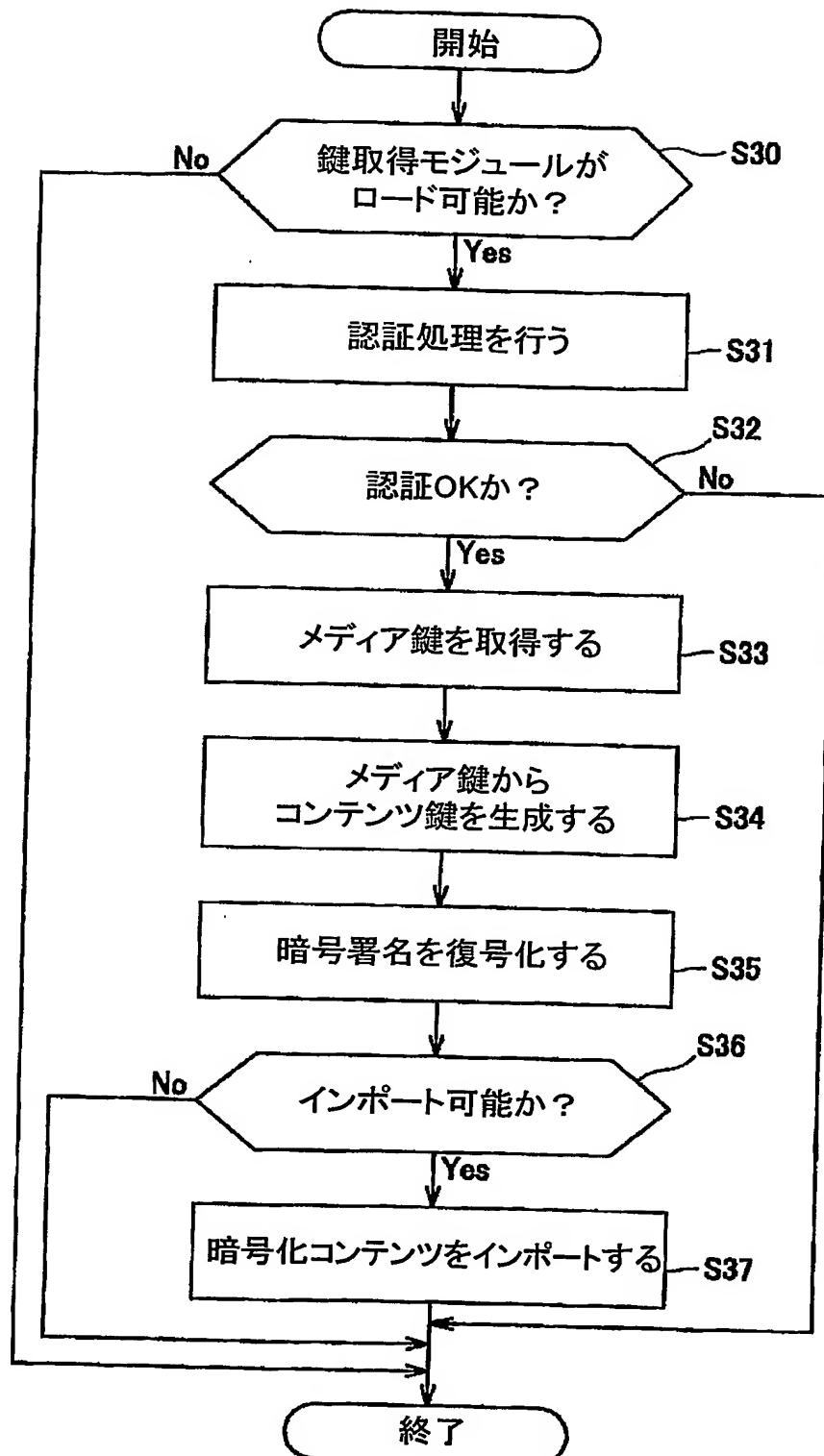


Fig.5

6/6

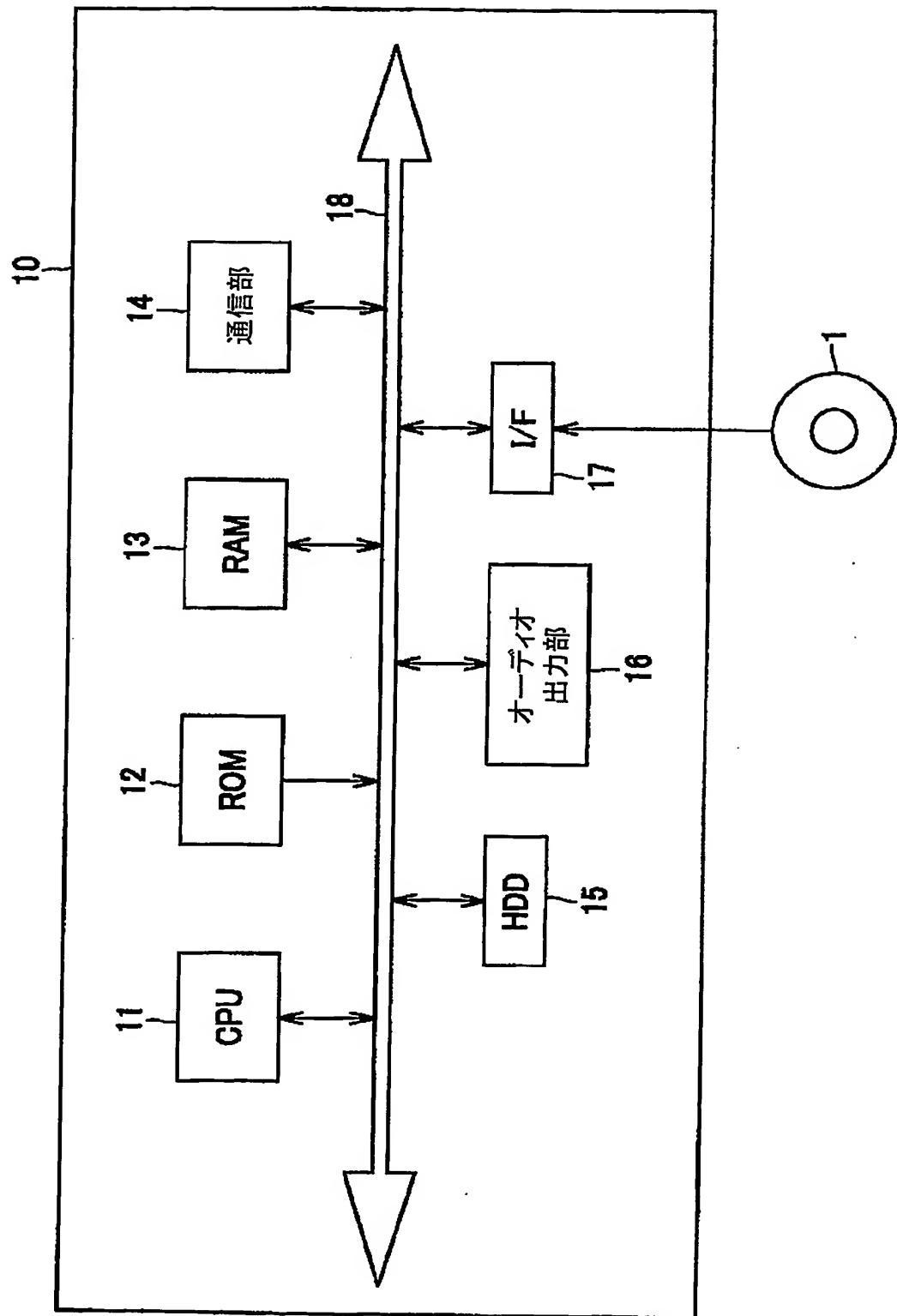


Fig.6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006900

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G11B20/10, 20/12, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G11B20/10-20/16, G06F12/14, G09C1/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-100116 A (Sony Corp.), 05 April, 2002 (05.04.02), Column 22, line 35 to column 23, line 32; column 25, line 47 to column 26, line 5; column 29, line 3 to column 30, line 43; column 31, lines 32 to 37; Figs. 1, 2, 5 to 8 & EP 1302944 A1 & EP 1302945 A1 & US 2002/157012 A1 & US 2002/184537 A1	1-8
Y	JP 2002-63075 A (Sony Corp.), 28 February, 2002 (28.02.02), Column 3, lines 26 to 32; column 5, lines 5 to 18; column 6, lines 1 to 7; Fig. 1 (Family: none)	1-8

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search
13 August, 2004 (13.08.04)Date of mailing of the international search report
31 August, 2004 (31.08.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.
Form PCT/ISA/210 (second sheet) (January 2004)

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/006900

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-14441 A (Matsushita Electric Industrial Co., Ltd.), 19 January, 2001 (19.01.01), Column 11, lines 19 to 47; column 14, line 34 to column 15, line 38; Figs. 5, 6, 9 & EP 1050887 A1 & EP 1304702 A1	4, 7
Y	JP 10-13403 A (NEC Corp.), 16 January, 1998 (16.01.98), Column 7, lines 21 to 41; column 9, line 23 to column 11, line 21; Figs. 1 to 5 (Family: none)	4, 7
Y	JP 10-123950 A (Fuji Xerox Co., Ltd.), 15 May, 1998 (15.05.98), Column 14, line 32 to column 17, line 12; column 23, line 1 to column 24, line 21; Figs. 1, 3 to 5, 18, 19 & EP 837383 A1 & US 6161183 A	4, 7
A	JP 11-250512 A (Sony DADC Austria AG.), 17 September, 1999 (17.09.99), Full text; Figs. 1 to 9 & EP 899733 A1 & US 6535858 B	1-8
A	JP 2001-229019 A (Toshiba EMI Ltd.), 24 August, 2001 (24.08.01), Full text; Figs. 1 to 9 (Family: none)	1-8

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl' G11B 20/10, 20/12, G09C 1/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl' G11B 20/10-20/16, G06F 12/14, G09C 1/00, H04L 9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2002-100116 A (ソニー株式会社) 2002. 04. 05, 第22欄第35行～第23欄第32行, 第25欄第47行～第26欄第5行, 第29欄第3行～第30欄 第43行, 第31欄第32-37行, 第1, 2, 5-8図 & EP 1302944 A1 & EP 1302945 A1 & US 2002/157012 A1 & US 2002/184537 A1	1-8

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

13. 08. 2004

国際調査報告の発送日

31. 8. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

早川 卓哉

5Q 9295

電話番号 03-3581-1101 内線 3590

C (続き) 関連すると認められる文献		関連する請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
Y	JP 2002-63075 A (ソニー株式会社) 2002. 02. 28, 第3欄第26-32行, 第5欄第5-18行, 第6欄第1-7行及, 第1図 (ファミリーなし)	1-8
Y	JP 2001-14441 A (松下電器産業株式会社) 2001. 01. 19, 第1.1欄第19-47行, 第14欄第34行~第15欄第38行, 第5, 6, 9図 & EP 1050887 A1 & EP 1304702 A1	4, 7
Y	JP 10-13403 A (日本電気株式会社) 1998. 01. 16, 第7欄第21-41行, 第9欄第23行~第11欄第21行, 第1-5図 (ファミリーなし)	4, 7
Y	JP 10-123950 A (富士ゼロックス株式会社) 1998. 05. 15, 第14欄第32行~第17欄第12行, 第23欄第1行~第24欄第21行, 第1, 3-5, 18, 19図 & EP 837383 A1 & US 6161183 A	4, 7
A	JP 11-250512 A (ソニー デーアーデーツェー オーストリア アクチングゼルシャフト) 1999. 09. 17, 全文, 第1-9図 & EP 899733 A1 & US 6535858 B	1-8
A	JP 2001-229019 A (東芝イーエムアイ株式会社) 2001. 08. 24, 全文, 第1-9図 (ファミリーなし)	1-8